Europäisches Patentamt

European Patent Office

Office européen des brevets

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

IB 2005/50594

Patentanmeldung Nr. **Patent application No.** **Demande de brevet n°**

04100708.9

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Europäisches Patentamt | European Patent Office | Office européen des brevets

Anmeldung Nr:
Application no.: 04100708.9
Demande no:

Anmeldetag:
Date of filing: 23.02.04
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method of encrypting a data stream

In Anspruch genommene Prioriät(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/ Classification internationale des brevets:

H04N9/79

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL
PT RO SE SI SK TR LI

Method of encrypting a data stream

Current legislation requires the possibility of encryption when storing television programmes received by broadcast. Television programmes, in particular digitally broadcasted television programmes, can be provided with copy control information as meta data. Options for the copy control information are among others: do not copy (recording not allowed), copy once (one recording allowed; copying recording not allowed) and copy free (free distribution of the content allowed within the personal environment of the consumer). And even when the copy free information is broadcasted with the television programmes, it may be required to encrypt any stored part of the television programme. This requirement is set in a further broadcast flag.

This requires implementation of encryption hardware and/or software in video recorders. The problem is, however, that the installed base does not support encryption. This can be solved by buying new equipment, but this is expensive. And on legacy equipment, legacy audiovisual material can still be reproduced. Furthermore, not all programmes recorded by video recorders with encryption functionality encrypt programmes when they record them. Besides that, the new video recorders with encryption functionality will be able to play back encrypted content. Therefore, it is not always directly necessary to discard the legacy DVD players.

However, as content on a DVD may be mixed, i.e. encrypted content is stored next to non-encrypted content, a user may try to playback encrypted content on a non-compliant DVD-player. With respect to reproduction of video data, this will result in not very interesting blocks on the screen. With respect to reproduction of audio data, this will result in noise, ticks et cetera, which can be quite loud. This is because not all audio data is encrypted; the first part of data packs stored on a DVD are in the clear and may comprise data which the DVD-player uses for synchronisation. The loud noise may damage equipment (speakers) and/or the ears of a user, especially when he or she wears headphones.

It is an object of the invention to solve or at least alleviate this problem.

To achieve this object, the invention provides in a first aspect the method according to claim 1.

When the ID of audio data is modified and not compliant with the DVD standard, a legacy player will not recognise the audio as such an will not reproduce any audio.

The invention will be further elucidated by means of Figures, wherein:

Figure 1 shows a video recorder 100 as an embodiment of the apparatus for storing data according to the invention;

Figure 2 shows a flowchart depicting an embodiment of the method for encrypting a data stream according to the invention;

Figure 3 shows a data pack produced by the method depicted by the flowchart shown by Figure 2; and

Figure 4 shows a DVD player as an embodiment of the apparatus for retrieving and rendering data according to the invention.

Figure 1 shows a video recorder 100 as and embodiment of the apparatus according to the invention. The video recorder 100 comprises a receiver 101, a de-multiplexer 102, a video processor 103 as a rendering unit, a coding circuit 110 as an embodiment of the circuit according to the invention, the coding circuit 110 comprising a multiplexer 104, an encryption unit 105 and a packet identifier unit 106. The video recorder further comprises a DVD recorder drive 107 as a storage device.

The operation of the video recorder 100 will be described by means of Figure 1 and a flowchart 200 as depicted in Figure 2, showing a recording process as an embodiment of the process according to the invention. The processes of the flowchart 200 are labelled as indicated in Table 1.

Reference numeral:	Label of process step
202	Start recording procedure, user input
204	Receiving data stream
206	[illegible]

206	Segmenting streams
208	Adding ID data to segments
210	Putting segments in packs
212	Sequencing packs
214	Encrypting packs
216	Alter ID data of basic audio stream segments
218	Store stream
220	End procedure

Table 1

The recording process starts by means of a user input in a process step 200. In a further embodiment, the recording process starts by means of an automatically generated input of a programming unit conceived to programme recordings by the video recorder 100.

Next, a data stream comprising data to record is received by the receiver 101 in a process step 202. The data stream can be received by receiving a signal 150 comprising the data by a wireless connection, a broadcast wired connection like cable, or a (virtual) point to point connection like broadband internet; various embodiments of the receiving process step 202 and the receiver 101 are possible. Having received the signal 150, the data stream is extracted from the signal and provided to the de-multiplexer 102. The extracted data stream is in this embodiment a transport stream comprising audio and video data streams for a television programme. In the further course of this description as well as the claims accompanying this patent application, both types of data will be referred to as audiovisual data, even when there is only audio or video data.

The de-multiplexer 102 separates the various audiovisual data streams comprised by the extracted programme stream to usually an elementary audiostream and an elementary videostream. A preferred format for these elementary streams is the MPEG-2 format. The programme stream may also comprise a stream with data for interactive television applications and a stream with data for enhancing the elementary audiostream and/or the elementary videostream. In Figure 2, the de-multiplexing process step is comprised by the receiving process step 202.

The elementary audiostream and the elementary videostream are provided to the video processor 103 for rendering the audiovisual data comprised by the elementary streams. For this description, rendering means that the MPEG-2 data (in case of the present embodiment) is decompressed and transformed for reproduction by a speaker 120 and a TV-set (not shown).

Besides rendering, the video recorder 100 is also capable of recording the received data. To this, the data received by the receiver 101 and de-multiplexed by the de-multiplexer 102 (both in the process step 204) is segmented in data segments in a process step 206. The data segments are also known as (data) packets.

Subsequently, ID data is added to the segments to identify the type of data comprised by the segments. The ID data identifies the type of data comprised by the segment and is pre-defined to facilitate playback of the stored data by a playback apparatus like a DVD (Digital Versatile Disc) player. For the DVD standard, the values of stream IDs as in Table 2 have been agreed. The ID data is comprised by a data segment (or data packet) header.

Table 2 also comprises information on sub stream IDs. Sub streams are comprised by a private stream comprised by the total data stream on a DVD. The sub streams provide further information, complementary to the basic audio and video data. Examples are AC-3, audio, DTS (Digital Theatre System), SDDS (Special Data Dissemination Standard), LPCM (Linear Pulse Code Modulation) and other.

	stream_id	sub_stream_id
MPEG Audio (base)	1100 0xxx	N/A
MPEG Audio (ext)	1101 0xxx	N/A
AC-3	1011 1101	1000 0xxx
DTS	1011 1101	1000 1xxx
SDDS	1011 1101	1001 0xxx
LPCM	1011 1101	1010 0xxx

Table 2

In a subsequent process step 210, the segments are arranged in data packs. Data packs comprise data segments of one type of stream. This implies that a data pack may comprise data of multiple sub streams. Optionally, data packs comprise a padding pack when not enough data of one stream is available to fill the 2 kB of the agreed data pack size. The packs are provided with a header for identification.

In a subsequent process step 212, the data packs with the audiovisual data are put in sequence in one data stream. This facilitates storage of the audiovisual data: when all the different streams that are provided simultaneously would have to be stored simultaneously, the DVD recorder drive 107 would require multiple writing units. These [illegible] used to [illegible]

Process steps numbered 206 through 212 form a sub process 230 which is carried out by the multiplexer 104. As a person skilled in the art will appreciate, these process steps may also be carried out by separate components.

After the packs have been put in one stream, they are encrypted in a process step 214. This encryption is done partly, so a playback apparatus is still able to read at least some data segment and data pack identification information of each pack. Preferably, the first 128 bytes of a data pack are not encrypted.

After the process step 214, data packs are obtained as depicted in Figure 3. Figure 3 shows a data pack 300, comprising a pack header 301, a data segment header 302 and a payload 320. The pack header 301 comprises data for identifying the data pack, the data segment header 302 comprises an ID segment 312 identifying the type of data comprised by the payload 320 (as set out in Table 2). The scramble information is comprised by two bits in the scramble identification bits 314.

In a subsequent process step 216, the ID data segment of data segments comprising audio data is modified. In this way, the audio packets are not recognised as such by a playback apparatus such as a legacy DVD player. This is done to prevent possible playback on a device that is not able to decrypt the packets. When a legacy DVD player, i.e. a DVD player not comprising an embodiment of the circuit of decryption according to the invention, would recognise an encrypted packet as comprising audio data, the legacy DVD player would try to playback the encrypted data. Usually, this will result in a lot of noise that could damage audio equipment such a speakers and, when played back over headphones, harm the ears of a user wearing the headphones.

When no audio data is recognised because the proper stream_id is not found, no audio will be played back and only decrypted video will be played back. This is not very interesting to watch, but does not harm the legacy DVD-player.

Inventors propose modification of the stream_id and sub_stream_id values as shown in Table 3. as a person skilled in the art will appreciate, modifications of this scheme are possible; Table 3 merely provides an embodiment.

	original		modified	
	stream_id	sub_stream_id	stream_id	sub_stream_id
MPEG Audio (base)	1100 0xxx	N/A	1100 1xxx	N/A
MPEG Audio	1101 0xxx	N/A	1101 1xxx	N/A

(ext)				
AC-3	1011 1101	1000 0xxx	1011 1101	1100 0xxx
DTS	1011 1101	1000 1xxx	1011 1101	1100 1xxx
SDDS	1011 1101	1001 0xxx	1011 1101	1101 0xxx
LPCM	1011 1101	1010 0xxx	1011 1101	11110xxx

Table 3

For the private stream, also the stream_id can be modified instead of the sub_stream_id. In Table 4, only stream_ids are modified, not the sub_stream_ids. Video, audio and sub_picture streams are now all hidden. An additional advantage of not including the sub_stream_ids is that it is not necessary to parse the stream to find the location of the stream ID, as it is always stored in the 18th byte of the pack.

	Stream_id	Modified stream_id	Comment
MPEG-audio base stream	1100 0xxx	1100 1xxx	Data mapped to valid MPEG audio streamnumber, not used by DVD (DVD streamnumer +8)
MEG-Audio ext stream	1101 0xxx	1101 1xxx	Data mapped to valid MPEG Audio streamnumber, not used by DVD (DVD stream number + 8)
Video stream	1110 0000	1110 1000	Data mapped to unused video stream number 15
Private stream 1 (used for AC-3, DTS, sub-picture, LPCM etc.)	1011 1101	1110 1111	

Table 4

Having modified the ID data of the audio stream of the data to store, the encrypted data packs are stored by the DVD recorder drive 107 in a process step 218. After all data has been stored, the process ends in a terminator 220 of the flowchart 200. It will be apparent to a person skilled in the art that altered ID data can also be added directly [illegible]

Figure 4 shows a DVD player 400 as an embodiment of the apparatus for rendering and retrieving audiovisual data according to the invention. The DVD player 400 comprises a DVD drive 401 as a storage device, a decryption unit 402, a de-multiplexer 403 and a video processor 404.

When playback of encrypted data stored on a DVD is requested, data is retrieved from the DVD by the DVD drive 401. Next, the packs are decrypted by the decryption unit 402. The de-multiplexer 403 is adapted to recognise modified ID data. This means that it is able to recognise data for the MPEG audio stream, even though the stream_id is different from what has been defined by the DVD standard. The decryption unit 402 and the de-multiplexer form a circuit 410 as and embodiment of the circuit for encrypting a data stream according to the invention.

The de-multiplexer forms elementary streams from the packets, delivering it to a video processor 404 for rendering to provide a signal that can be reproduced on a speaker 420 or a TV-set (not shown). The video processor can be embodied as a MPEG decoder.

CLAIMS:

1. Method of encrypting a data stream comprising at least one stream of audiovisual data, comprising steps of:

(a) segmenting the stream of audiovisual data in data segments;

(b) providing the data segments with ID data in an ID segment, the ID data being different from ID data being pre-determined to identify the type of data in the stream of audiovisual data; and

(c) partly encrypting the data segments, leaving the ID segment unencrypted.

2. Method according to claim 1, wherein the method further comprises the step of creating data packs, each data pack comprising at least one data segment and wherein in the step of partly encrypting the data segments, the ID segment of at least on data segment is unencrypted.

3. Method according to claim 1, wherein the data stream comprises multiple streams of different types of audiovisual data and data segments of at least one stream of audiovisual data are encrypted

4. Method according to claim 3, wherein data segments of at least on stream of audiovisual data is provided with ID segments comprising ID data being different from ID data being pre-determined to identify the type of data in the stream of audiovisual data.

5. Method according to claim 3, wherein the multiple streams of audiovisual data are provided simultaneously and the method further comprising the step of multiplexing the segments comprising data of the multiple streams of audiovisual data to a further data stream.

6. Method according to claim 1, wherein the data segments are provided with further ID data in the ID segment, the further ID data being pre-determined to identify the type of data in the stream of audiovisual data and the further ID data being in a further step

replaced by the ID data being different from ID data being pre-determined to identify the type of data in the stream of audiovisual data.

7. Method of storing a data stream comprising at least one stream of audiovisual data, comprising the step of receiving the data stream, the method as claimed in claim 1 and the step of storing the segmented and encrypted data on a storage medium.

8. Circuit for encrypting a data stream comprising at least one stream of audiovisual data, comprising:

(a) a segmenting unit for segmenting the stream of audiovisual data in data segments;
(b) providing the data segment with ID data in an ID segment, the ID data being different from ID data being pre-determined to identify the type of data in the stream of audiovisual data; and
(c) an encryption unit for partly encrypting the data segments, leaving the ID segment unencrypted.

9. Circuit according to claim 8, further comprising a packing unit for creating data packs, each data pack comprising at least one data segment; and wherein in the step of partly encrypting the data segments, the ID segment of at least on data segment is unencrypted.

10. Apparatus for storing data, comprising:

(a) a receiver for receiving data;
(b) the circuit according to claim 8; and
(c) a storage device for storing the encrypted data on a storage medium.

11. Method of decrypting audiovisual data encrypted using to the method as claimed in claim 1, comprising the steps of:

(a) decrypting the partly encrypted data segments;
(b) recognising that the data carried by the ID segment is different from ID data being pre-determined to identify the type of data in the stream of audiovisual data and recognising the actual type of data comprised by the data segment; and
(c) forming a stream of audiovisual data from the data segments.

12. Method of retrieving an rendering data stored using the method as claimed in claim 7, comprising the step of retrieving data stored on the storage medium, the method as claimed in claim 11 and the step of rendering the decrypted stream of audiovisual data.

13. Circuit for decrypting audiovisual data encrypted by the circuit as claimed in claim 7, comprising:

(a) A decryption unit for decrypting the partly encrypted data segments;

(b) An identification unit for recognising that the data carried by the ID segment is different from ID data being pre-determined to identify the type of data in the stream of audiovisual data and recognising the actual type of data comprised by the data segments; and

(c) A streaming unit for forming a stream of audiovisual data from the data segments.

14. Apparatus for rendering and retrieving audiovisual data, comprising:
a storage device for retrieving data from a storage medium;
the circuit according to claim 12; and
a circuit for rendering the decrypted stream of audiovisual data.

15. Computer programme product comprising computer readable instruction for programming a processing unit for executing the method according to claim 1.

16. Data carrier carrying the computer programme product as claimed in claim 1.

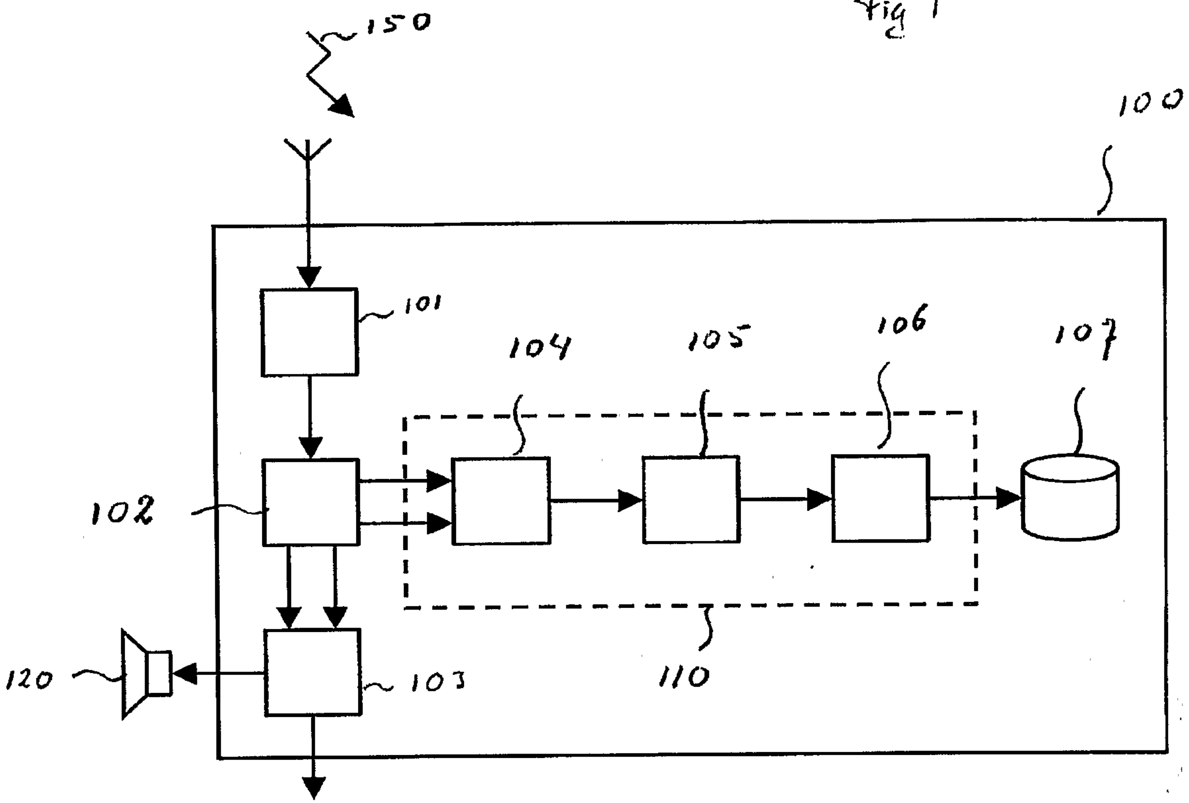
17. Programmed computer enabled to execute the method according to claim 1.

18. Computer programme product comprising computer readable instruction for programming a processing unit for executing the method according to claim 11.

19. Data carrier carrying the computer programme product as claimed in claim 11.

20. Programmed computer enabled to execute the method according to claim 11.

Fig 1


150
100
101
104
105
106
107
102
110
120
103

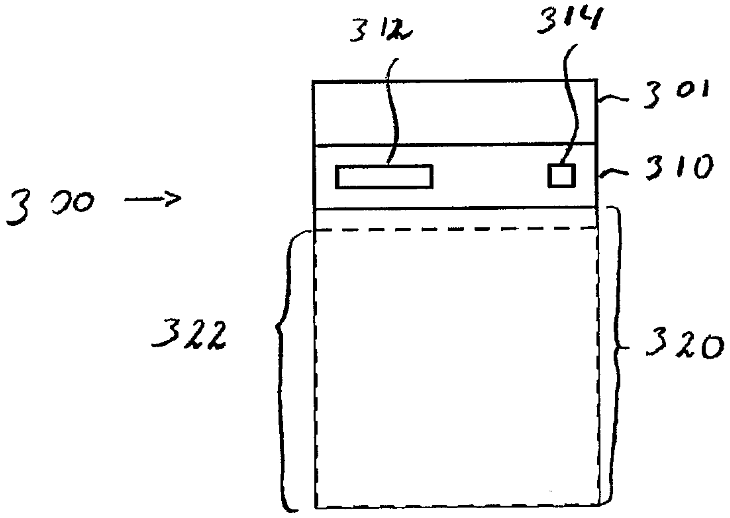

312
314
301
310
300
322
320

Fig 3

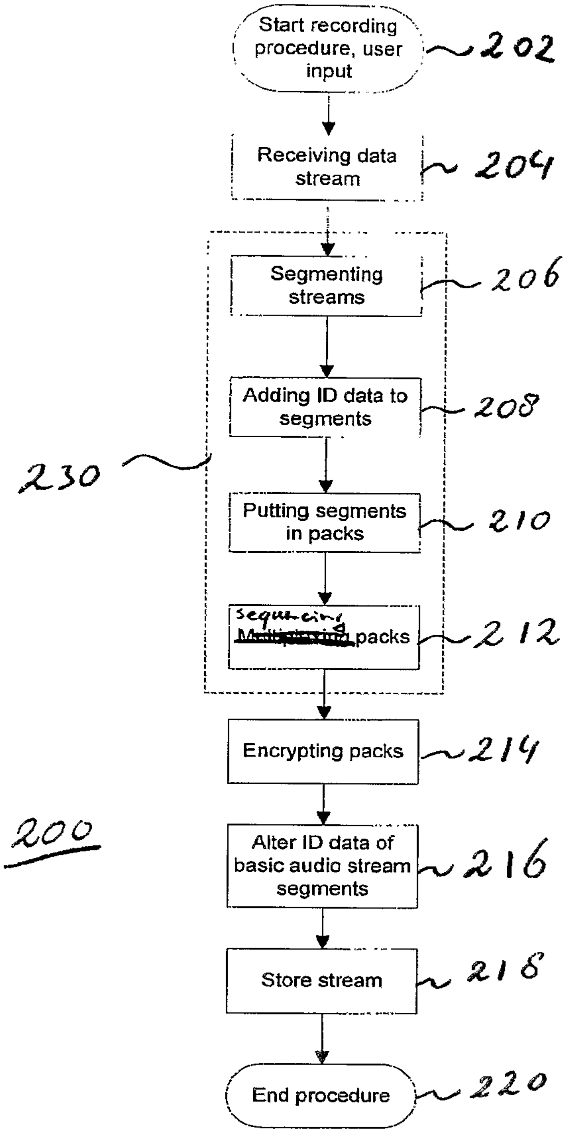


Fig 2

⇒ tekst graag verwijderen uit figuur.

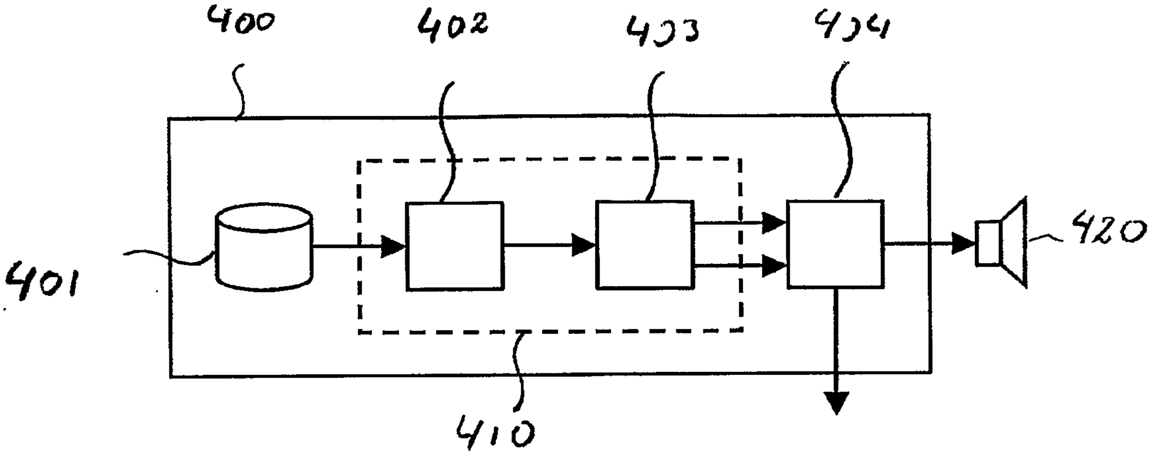


Fig 4